Computer Security Strategies: An Instructional Design Approach

Adam Tanare Jr.
University of Hawai'i at Manoa
1776 University Avenue
Honolulu, HI 96822
United States
tanare@hawaii.edu

Abstract: Computer security can be an overwhelming concept for a technology layman or digital immigrant. However, recent occurrences of cyber-attacks highlight that computer security is an essential practice that remains neglected. In this instructional design study, a web-based hybrid text/computer game module was designed based on the ARCS model to examine its effectiveness in teaching basic computer security strategies to sixth graders. Two face-to-face pilot study sessions were conducted for field evaluation. Revisions were made based on feedback and observations, and a small group evaluation was conducted face-to-face, yielding 22 valid participants. Results found that 10 of 12 learning objectives saw an increase in average participant knowledge from pre-test assessment to post-test assessment. Participants expressed that the lesson was fun and informative. Participants were observed to be deeply engaged in the lesson, particularly during the scored game sections. A majority of discussion includes best practices, and details the value and impact of the pilot studies' findings in systematically improving the effectiveness and relevance of instruction. Findings will be used to further refine the module for possible instructional deployment or commercial use. Potential for a longitudinal study exists, and would examine the longstanding effects, if any, the lesson exhibited on participants.

Introduction

Computer-driven technologies have proliferated at an exponential rate in the last decade. Our cell phones and laptops are becoming televisions, Internet providers, and communication devices. All users of technology regardless of skill level should maintain good security practices. Yet, multiple cyber-attacks continue to occur which reveal that many lack both the understanding and application of basic computer security. Educational computer games could be more effective than traditional methods of teaching such topics, particularly to a younger audience. Use of multiple instructional design concepts can further enhance the value of instruction. Thus, the purpose of this instructional design project was to develop and evaluate a hybrid web-based text/computer game instructional lesson for sixth graders that can teach the importance of using multiple computer security strategies.

Background

The need for stronger computer and online security practices are evident in the details behind many of the prolific cyber-attacks that occurred on the Internet in 2011. No attack was more prominent than the one that affected Sony's PlayStation Network (PSN) and possibly all of its account holders numbering around 77 million, at the time (Purchese, 2011). An analysis of data released online by the alleged hackers, including user-names and passwords (Mills, 2011), suggest that many users are either unaware of good security practices, are poor at it for various reasons, or are simply negligent (Rapoza, 2007).

Password Security

Unauthorized data that was released from a related Sony Pictures cyber-attack and an earlier cyber-attack on the website Gawker was analyzed for password length, variety of character types, randomness, and uniqueness (Hunt, 2011). In short, it was found that an alarming amount of users used poor passwords that could be easily guessed by hackers and/or software in a direct attempt to gain access to a computer or online account. Furthermore, analysis of user accounts found on both breached data-sets indicated that a majority of these users re-used their user-name, email, and/or password between both accounts. Poor passwords that are reused across accounts are a major security risk for all computer users ("Practical advice", 2011) and opens up a high possibility of secondary attacks (Stevens, 2011).

Software Updating

Software updating is a critical process of all computer systems regardless of operating system ("The irrepressible", 2010). Computers with outdated computer and system software are extremely vulnerable to malicious exploits that are propagating the Internet on questionable websites (i.e., file-sharing, gambling, etc.) and even on some reputable websites that may have been compromised.

Online Security

Many exploits are made possible when users click on malicious hyperlinks that propagate as a result of a Search Engine Optimization (SEO) poisoning attack (Howard and Komili, 2010). Identity theft or loss of access to user accounts on social networking sites like Facebook may occur if users enter and submit their user-name, emails, and password credentials onto websites that do not provide Secure Socket Layer (SSL) or Hypertext Transfer Protocol Secure (HTTPS) security. Many more attacks are made possible through hyperlinks that propagate on Facebook wall posts, and designed to lure unsuspecting teens to dangerous websites hosting phishing and malware attacks (Hua, 2011).

Relevant Research

Age Rationale

Age has been linked to risky behavior, as a result of their (adolescents) processes in learning about the world (Reyna & Farley, 2006; as cited in Sheng, Holbrook, Kumaraguru, Cranor, and Downs, 2010). Research has shown that individuals between age 18 and 25 are more susceptible to phishing attacks, compared to other older age groups (Sheng, et. al., 2010). Reasons cited include, "lower levels of education, fewer years on the Internet, less exposure to training materials, and less of an aversion to risks" (Sheng, et. al., 2010, p2). Education that can help alleviate this risk factor would be beneficial to adolescents before they come of that age.

Video Game Medium

Video games can serve as a unique medium for teaching and learning, especially for the most abstract of concepts. In 2009, Wombat security is one such firm that has commercialized a computer game called "Anti-Phishing Phil" to teach work personnel how to recognize phishing emails, a major computer security threat. Utilizing graphics more suitable for young children, players control a swimming fish who must hunt for worms, while evaluating whether or not to eat it based on a legitimate or fraudulent hyperlink that appears (Cronin, 2009). Wombat has said that their game has been shown to be significantly more effective at training personnel to recognize phishing attacks than more traditional training solutions ("Computer game", 2009).

Theoretical Frameworks

Considering for possible difficulties a young audience may have with a concept as difficult as computer security, motivation and relevance were anticipated as major factors in the design process. Educators at all levels face the challenge of stimulating learner motivation and finding effective methods for motivating learners (Keller, 1999, cited in Keller, 2000). Keller's ARCS model of attention, relevance, confidence, and satisfaction influenced the design of the web-based module.

Purpose of Project

The purpose of the project was to create an instructional design module that would make the task of teaching basic computer security concepts more engaging and relevant to children.

Thus, a computer game medium was decided upon as a unique medium that could engage young learners and teach computer security concepts that would otherwise be difficult to understand. It was expected that the computer game format would be novel and fun for participants, and would enable them to learn in a modality that was different from a traditional classroom instruction model.

Target Audience

The instructional design module was developed for sixth grade students from a Honolulu, Hawaii charter school. Participation was open to any student in the sixth grade level who could complete a consent form (parents) and assent form. Due to logistical restraints, only about 30 overall students participated, of which 22 made up the valid data set. This age group was selected because they have not likely learned any of the cyber-security content taught in the module, but has likely experienced video gaming in some form. They are also more likely to be victimized by online threats due to inexperience and naiveté.

Module Design

A web-based hybrid text/computer game module was created, where instruction and learning content was present in both the text portion and computer game portion. This format lends well to the audience, who are digital natives who are accustomed to such technologies like Google Docs and MacBook computers in their regular curriculum.

The module contained a demographics survey, pre-test assessment, embedded tests contained within two computer games sections, post-test assessment, and attitudinal survey. All data collection tools utilized Google Forms, and the incoming data was collected in Google Docs. Instruments used within the surveys included multiple choice, questions with multiple correct answers, likert scales, 10-point scales, and open-ended response.

The module was partitioned into two sections, spanning 19 separate web pages. Section one covered password and computer security, while section two covered online security (Table 1). An embedded test concluded each section, and was based within two computer games authored by the researcher.

Navigation through the website was linear, and participants could only advance through the module by using navigational links at the bottom of each page. Participants spent time reading informational content on each page before proceeding. Once participants reached the end of a section, they could play a computer game to reinforce and practice the content they've learned. The combination of instruction through web-based text and images, with interactive computer game sections was by design; participants would be motivated to progress through the instructional module so that they could continue to play the computer games. Meanwhile, all necessary learning content was present in both the webpages and the computer games to ensure multiple ways of acquiring content knowledge. It was also meant to make sure that even if participants skipped informational content during the computer games, for whatever reason, they had covered it in the text of the module web pages.

Technologies

All instruction was based within a website created with Weebly, an online website creation service. Due to the target audience school site having only Apple laptops, GameMaker HTML5 was purchased for $99 and was used as the game authoring

software of choice because the compiled game (end-product) was web browser dependent rather than operating system dependent.

Computer Game

Two computer games were built to engage the participants while learning. Both were simple maze games where participants had to navigate their character, SPADE (Strong Password Augmenter Defense Energizer) to the exit while avoiding malicious threats like viruses, malware, Trojan horses, worms, and keyloggers, all of which could hurt or destroy SPADE. Participants quickly learned that they needed to collect every 'password powerup' on a 'maze level' in order to destroy all the malicious threats that stood in their way of the exit. Password powerups used graphics that resembled characters, numbers, symbols, and uppercase and lowercase letters (Fig. 1); this was to help enforce several learning objectives that taught the importance of using a variety of these in a password.

Fig. 1. Password Powerups Graphics

The maze levels were designed to feature a natural progression of difficulty. Game elements were introduced one-by-one in a similar fashion. A software update powerup was introduced half-way through the first game to enforce the importance of software updating, which was covered in section one of the module; this powerup was blocked by threats and could only be reached by collecting all other password powerups. Collecting the software update powerup destroyed keyloggers that were not destroyed by collecting the other powerups. A lock powerup was introduced early in the second game, which granted the player character invincibility and was meant to enforce the concept of SSL and HTTPS security.

'Load screens' (i.e., a screen where players have limited or no control/input during the game) were placed during the transitions between maze levels and displayed text and images that taught participants how to play the game or provided a quick review of instructional content. 'Quiz rooms' appeared frequently in-between maze levels and load screens, and served as the embedded test for participants to practice and learn (Fig. 2). Participants could not leave this room until they had selected the correct answer. To encourage participants to answer correctly, points for correct answer(s) were worth much higher than points attained by collecting password powerups. Participants were penalized with a score reduction for selecting the wrong answer—this mechanic discouraged participants from randomly choosing answers just to exit the room.

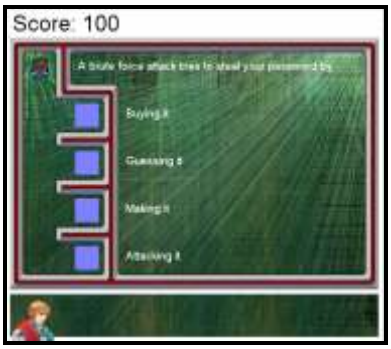

Fig 2. Quiz Rooms

Load screens that explicitly gave the correct answer for an upcoming quiz room were placed *before* a level to allow for time to pass; if these were placed directly prior to quiz rooms, students could easily exploit the game by simply recalling the answer they have recently seen, rather than actually learning.

Progression of levels in computer games:
Load Screen [game info or instructional content] > Maze Level > Quiz Room, (repeat)

Methods

With help from several school faculty members, two pilot studies were scheduled and conducted to gather critical feedback from the target audience on February 7 and 9, 2012. The pilot study was required to gauge how long the study would take for a large audience. Four participants in each pilot study session (of which only one was male) were provided a handout where they were asked to self-monitor their progress and satisfaction level throughout the module. They were asked to list the approximate time spent in each section listed, as well as provide feedback. Dialogue was encouraged, and the environment of the pilot study was similar to an open forum or focus group. Afterwards, revisions were made to all sections of the instructional module, and a small group evaluation was conducted on February 16. Procedures were the same for both the pilot study and the small group evaluation, however the latter was treated more like a closed-room exam than an open forum. Within the valid set of participants in the small group evaluation, nine were males and thirteen were females. While the module was completely web-based, instruction, supervision and observation was made possible due to the face-to-face setting of a supervised classroom.

Results

The main focus of the small group evaluation was to see if the improvements made from feedback from the pilot study helped improved the effectiveness of the module. To that end, results were analyzed from a valid set of 22 participants, omitting any students in the small group evaluation who had also participated in the prior pilot study sessions. A total of 12 questions were present in the pre-test, embedded-test, and post-test. The embedded-tests occurred within the computer games and could not be recorded. Results show a

positive increase from pre-test to post-test for all but two questions. While the pre-test scores had only two questions over the 70% correct range, the post-test had seven. The scores may also suggest that section one was better structured and helped students gain a better understanding of password security; section two was perhaps less structured and more ambiguous; scores were not as high as section one.

Table 1. Pre-Test and Post-Test Assessment Scores

Question Number and Learning Objective (N=22)	Pre-Test	Post-Test
Section 1: Password Mishaps		
1. Brute Force Attack	41%	86%
2. Password Strength	64%	77%
3. Keylogger	18%	77%
4. Password Memorization	45%	86%
5. Password Makeup	73%	100%
6. *Software Updates	23%	32%
Section 2: Online Security		
7. **SSL: Secure Socket Layer	45%	64%
8. **HTTPS: Hypertext Transfer Protocol Secure	50%	27%
9. Purpose of SSL & HTTPS	5%	23%
10. *Location of Security Information in Browser(s)	5%	0%
11. **SEO: Search Engine Optimization	77%	86%
12. Revealing Hyperlink Address	14%	73%

**Denotes a question that had more than one possible answer*
***Denotes an objective that asked students to memorize an acronym*

Question Difficulty

Several questions saw low overall scores between pre-test and post-test despite general improvement. In particular, questions that required more than one correct answer saw scores below 32%. It may not have been clear to participants that they had to select more than one answer, and the question itself may have been confusing, in comparison to other simpler questions that scored higher. Questions that were acronyms scored fairly low with the exception of SEO (Search Engine Optimization). Students at the 6th grade level probably struggle to memorize acronyms; HTTPS and SSL are as unattractive an acronym as PEMDAS in mathematics. Furthermore, in the small group evaluation revision of the module, HTTPS and SSL were presented as simple acronyms with little to no background or context surrounding it. As for SEO scoring highly, the distractor items were too easy and were giveaways, and coincidentally, the correct answer was listed as the first item. The possibility exists that participants were simply exhausted by the time they reached section two, and performance suffered as a result; the entire module on average took over an hour to complete.

Discussion

The decision to utilize a computer game within the module was a preconceived idea that ended up having a significant effect on the implementation. Open ended feedback from participants was resoundingly positive regarding the computer games. One participant said, "*I liked that it (the module) was very educational and not very boring, like most educational games.*" Another participant said "*I just liked every part of it (the module). Because it was both challenging and fun."* The pilot studies were instrumental in improving the overall relevance and effectiveness of the module for the small group evaluation participants.

Pilot Study: Observations and Improvements

Assessing participant knowledge levels was a difficult task throughout the entire development process, but was made much easier through data and feedback received from the pilot study sessions. Overabundance of reading was a common complaint that many recommended be fixed.

Thus, revisions to the module and computer games were focused on making the content more youth-friendly and greatly reducing the cognitive load. A tremendous amount of words, sentences, and paragraphs were removed, and even an entire section dedicated to computer accounts was scrapped. Simplified sentences were used, and were accompanied by cartoon images that were entertaining but not necessarily relevant to the instruction. Computer game load screens containing instructional content that displayed lengthy informational paragraphs were scrapped in favor of screens that simply displayed the correct answer for the upcoming quiz room (Fig.3).

Fig 3. Load Screens: Pilot Study and Small Group Evaluation Versions

Assessing and adjusting for participant motivation was another challenge. Participants in the pilot study were observed looking uninterested in the module. However, once they reached the first computer game, their interest level was suddenly invigorated and they were engaged in the module the rest of the way.

During the pilot study, participants spent a large amount of time on surveys, particularly the initial demographic survey and pre-test assessment. Participants continually asked for clarification for pre-test questions, many times asking out loud for the answer to the question itself. Participants had to be reminded to treat the test portions as a class exam and that they simply had to try their best. Prior explanation of the purpose and progression of the instructional module would have alleviated many problems including time delays, and was implemented to some extent in the small group evaluation.

Another area that saw significant time delays were the computer games. Participants were not deterred by constantly dying in the maze levels; they had fun and refused to skip the levels when given the opportunity. Compounded by the need to have an IT specialist unblock the content filters on one of the pages that contained the word 'hacking', serious time delays hampered completion times. An overhauled game engine was created in response to these observations, and was also necessary because the project file had become corrupted shortly after the first pilot study. The revised computer games were much easier; SPADE could now sustain up to four hits from threats before dying, threats were made to move slower. Finally, an automatic level skip feature was implemented so that participants were forced by the game to skip after dying on a level two times. Of note, the level skip feature was one of a few features introduced into the game as a result of feedback from participants in the attitudinal survey.

Conclusion

The instructional design module could be considered a success, but leaves a lot of room for improvement in all phases. A better effort in analyzing and understanding the 6th grade audience's skill levels would have saved a lot of time during module development. The pilot study proved instrumental to making a more successful lesson for participants during the small group evaluation. Open-ended response feedback suggests that the selection of a hybrid web-based text/computer game module was the right one for the target audience. One major factor that needed to be addressed at all times was participant motivations. Much more can be done to improve the module for future studies, or even instructional deployment. Commercial development is also possible. A possibility for a longitudinal study exists, which could examine participants' growth in knowledge levels and if they have been applying the concepts effectively.

References

Computer game deployed to combat phishing. (2009). *UPI Security Industry*. Retrieved from Newspaper Source Plus online database.

Cronin, M. (2009, October 20). U.S. State Department buys Internet security software from Oakland firm. *Pittsburgh Tribute Review (PA)*. Retrieved from Newspaper Source Plus online database.

Howard, F., Komili, O. (2010). Poisoned search results: How hackers have automated search engine poisoning attacks to distribute malware. Retrieved from http://www.sophos.com/en-us/why-sophos/our-people/technical-papers/sophos-seo-insights.aspx

Hua, V. (2011). Redefining the security wall. *THE Journal*, 38(7), 36-38.

Hunt, T. (2011, June 6). A brief Sony password analysis. Retrieved from http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html

Keller, J. M. (1999). Using the ARCS motivational process in computer-based instruction and distance education. *New Directions For Teaching & Learning*, (78), 39.

Keller, J.M. (2000). How to integrate learner motivation planning into lesson planning: The ARCS model approach. Retrieved from http://mailer.fsu.edu/~jkeller/Articles/Keller%202000%20ARCS%20Lesson%20Planning.pdf

Mills, E. (2011, May 18). Expert: Sony attack may have been multipronged. Retrieved from http://news.cnet.com/8301-27080_3-20063789-245.html

Practical advice on choosing good passwords (2011, August 15). Retrieved from http://lisnews.org/practical_advice_choosing_good_passwords

Purchese, R. (2011, May 5). Kaz Hirai's full letter to Congress. Eurogamer.net. Retrieved from http://www.eurogamer.net/articles/2011-05-05-kaz-hirais-letter-to-congress-in-full-blog-entry_2

Rapoza, J. (2007, May 7). Twelve ways to be a security idiot. Retrieved from Academic Search Premier online database.

Sheng, Holbrook, Kumaraguru, Cranor, Downs (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectives of interventions. Retrieved from http://lorrie.cranor.org/pubs/pap1162-sheng.pdf

Stevens, N. (2011, June 18). Tech at Night: Reusing passwords is dangerous, wireless competition is strong, defunding net neutrality, copyright overreach. Retrieved from http://www.redstate.com/neil_stevens/2011/06/18/tech-at-night-reusing-passwords-is-dangerous-wireless-competition-is-strong-defunding-net-neutrality-copyright-overreach/

The irrepressible reasons for upgrading software (2010, Mar 12). Retrieved from http://www.itomic.com.au/article/The-Irrepressible-Reasons-for-Upgrading-Software